Business Interruption And Loss Of Assets Risk Assessment In Support Of The Design Of An Innovative Concentrating Solar Power Plant

Andrea Amato, Michele Compare, Maurizio Gallisto, Augusto Maccari, Mauro Paganelli, Enrico Zio

Business interruption and loss of assets risk assessment in support of the design of an innovative Concentrating Solar Power plant

Andrea Amato[2], Michele Compare[1], Maurizio Gallisto[2], Augusto Maccari[2], Mauro Paganelli[2], Enrico Zio[1,3] *

[1] Energy Department, Polytechnic of Milan, Milan, Italy

[2] Techint - Compagnia Tecnica Internazionale SpA, Milan, Italy

[3] Ecole Centrale Paris - Supelec, Paris, France

*Corresponding author: enrico.zio@polimi.it, enrico.zio@ecp.fr, enrico.zio@supelec.fr

Abstract: Concentrating Solar Power (CSP) plants are a promising technology of renewable energy production, as witnessed by the increasing public and private investments during the last decade. The assessment of the associated risks of business interruption (loss of production) and loss of assets due to the occurrence of undesired internal or external events, such as failures of components, unfavorable environmental conditions, etc., brings added values by informing design modifications and contributing to production assurance, for rational Company investments in these environmentally sustainable power plants. This work presents and applies a methodology for assessing the risks associated to a CSP of innovative design. The methodology is derived from traditional system risk analysis, specifically focused only on the economic consequences of the internal events of failure behavior of components. The innovation in the design considered is particularly aimed at augmenting the CSP intrinsic capability of being equipped with thermal storage systems by the introduction of a molten salt mixture as heat transfer fluid. This technology presents evident advantages in terms of system simplification and reduction of production costs but on the other hand introduces a risk factor with regards to the solidification of the salt mixture that occurs at about 240°C.

Keywords: Concentrating Solar Power plant, Molten Salt Mixture, Hazard Scenarios, Hazard Identification (HAZID) Analysis, Quantitative Risk Analysis, Business Interruption, Loss of Assets.

1 Introduction

In the current scenario of global warming and global competition in the energy market (mainly driven by the limited availability of fossil fuels), in the last years a growing attention has been paid to the renewable energies and associated technologies, by both politics and the scientific community worldwide. In this context, the European Union (EU) commission presented in 2007 a strategic overview on the European Energy Policy measures, which puts particular emphasis on the use of renewable energies and on the development of new technologies to exploit the potential of alternative energies, with the objective of reducing the dependency on energy import, boosting industrial competitiveness and promoting economic and social development [1]. In the report, the EU commission identifies the CSP technologies as potentially significant contributors to the development of a more sustainable energy system, predicting that these technologies will play a key role in meeting the target of supplying 20% of the total EU energy demand by renewable energies. Coherently with this vision, the EU commission has been supporting research in CSP technologies for several years, with notable results, and established new specific funding instruments for support of their development [2]. This has led to the design and building of a number of pilot plants with

different technological solutions in different parts of South Europe and North Africa, some of the most 'solar-fit' regions of the World.
Although the technological developments are encouraging, the full growth of CSP plants is still undermined by a number of practical aspects, the most important being the relatively high final cost of produced energy that limits the competitiveness of such plants. In view of this challenge, Techint-Compagnia Tecnica Internazionale (in the following referred to as Techint) embraced an innovative and promising CSP technology (based on a technology development program carried out by Ente Nazionale per le Nuove Tecnologie l'Energia e l'Ambiente, ENEA), which is expected to guarantee higher power generation performances than those of other competing CSP technologies. Based on the analysis of this technology, Techint is prepared to invest in the development and construction of these plants for commercial exploitation.

The strategic direction of investment calls for the rational answer to three questions:

- How will the plant actually perform?
- How can one guarantee the reliability/availability requirements?
- Is the development risk sustainable from the economic point of view?

The first question arises naturally from the general uncertainty on the success of novel technologies, due to lack of experience and the too few lessons that can be learnt from little similar operating plants. To address this question, a scaled-down pilot plant has been designed and is planned to be built on the site of Massa Martana (Italy); the observed generation performances of the pilot plant are expected to contribute to reducing the uncertainties on the selected technology, increasing the Company confidence on the economic viability of the investment program.

The answer to the second question requires the development and application of Reliability, Availability and Maintainability (RAM) analyses, taking into account the peculiarities of the plant and the characteristics of the site of installation. With respect to the latter, in fact, the Company investment program foresees to build a number of plants in different regions of the South Mediterranean area, characterized by different environmental conditions.

The answer to the third question is the focus of the work presented in this paper, which reports about the research activity carried out in collaboration between Politecnico di Milano and Techint, for the development and application of a methodology for identifying and assessing the economical risks associated to the CSP plant operation, related to the occurrence of undesired events to its components.

The paper is organized as follows. Section 2 briefly recalls the essential notions about the CSP technology selected by Techint. Section 3 provides a description of the risk assessment methodology and the results of the application of this methodology. Some concluding remarks and perspectives for future advancements are given in the last Section.

2 The selected CSP technology: X-ITE® trough parabolic collectors

The CSP plants, often also called Solar Thermal Power (STP) plants, can be divided into four classes: Fresnel Systems, Solar Towers, Dish/Engine Systems and Parabolic Troughs. All these plants produce electricity in much the same way as conventional power stations. The difference among them is that they obtain their energy input by concentrating in different ways solar radiation, and converting it to high-temperature steam or gas, which then drives a turbine or motor engine. Differently from other solar technologies, the CSP plants can keep working at a constant load thanks to the thermal storage systems, whose main function is equivalent to that of the fuel in other power generation systems. This potentially

leads to an optimal plant utilization with higher margins and shorter return of the investment, making the CSP technology particularly attractive for investors.

The CSP plant type selected by Techint is based on the conventional parabolic trough, enhanced by innovative design solutions. Figure 1 provides a schematic view of the reference plant and of its key components: mirrors, receivers, thermal storage system and turbine. Roughly speaking, a parabolic solar collector tracks the Sun continuously and exploits the optical properties of the parabolic mirrors, which reflect the incident parallel rays in the optical focal line, to concentrate the Sun's rays onto a heat absorber element (the 'receiver' in Figure 2). The solar radiation warms up the heat transfer fluid flowing through the absorber tube (up to 550°C in the reference plant), and the hot salt mixture is accumulated in the hot tank (this is technically called the 'thermal storage charging phase', during which the level of the cold tank is reduced and the level of the hot tank is increased). When the delivery of electric energy is required a molten salt flow is spilled out from the hot tank, the fluid is conducted along a heat exchanger in which steam is produced and finally the cooled molten salt flow is re-collected in the cold tank (this is technically called the 'thermal storage discharging phase': dually from the previous charging phase, the level of the cold tank is increased and the level of the hot tank is reduced). The produced steam generates rotating power in the turbines, which is converted in electrical power with an expected output of about 10-50 MW of electricity, depending on the rate design of the plant.

The receiver adopted in the reference CSP plant represents a fundamental technological innovation, patented by ENEA and consisting of a specially coated absorber tube (solar absorbance of 95% and emissivity of 10% at 400°C) which is embedded in an evacuated glass envelope; the high photo-thermal properties allow achieving an high working temperature (580°C) and consequent high efficiency of the plant, with high mechanical reliability.

The reflecting panels are also novels; they are made of a thin glass-silvered mirror coupled to a supporting panel in Sheet Moulding Compound (SMC); this solution combines the advantages of the glass mirror (a cheap and reliable reflecting material) with the improved mechanical properties of composite materials.

Last but not least, also the heat transfer fluid is an innovative solution; it is a molten salt mixture (60% $NaNO_3$ - 40% KNO_3) operating at temperatures in the range of 290-550°C, assuring chemical stability up to 600°C and which does not contribute to the degradation of the tubes. This innovation leads to several important aspects: the increase of the operating temperature from 390°C up to 550°C, with an increase of the thermodynamic efficiency; the reduction of storage costs consequent to system simplification and reduction of storage media inventory for the same amount of storage capacity; the reduction of the environmental impact of such kind of plants.

3 Assessment methodology

The methodology developed to assess the plant power generation performance is based on the framework of system risk analysis, focused on business interruption (loss of production) and loss of assets only (in other words, safety consequences are not considered).

The analysis is made up of three main phases, which are detailed in the next sub-Sections:

- modeling of the plant (its components, systems and functions);
- hazards identification and failure analysis: the identification and analysis of the 'hazardous' events/processes/parameters which may lead to assets losses and/or business interruptions;
- quantitative analysis of accident scenarios leading to loss of production and assets.

3.1 Modeling of the plant

A full understanding of the engineering system to be analyzed is the first step of the methodology. Two techniques have been employed (further details about them can be found in [3]-[7]):

- Block Diagram: a schematic representation of the hierarchical and logical relations linking the physical elements of the plant at any level of detail (also referred to as indenture level [5]; e.g., systems, subsystems, items).
- Functional Analysis: a break down of the system functions through the different levels of detail; i.e., functions at indenture level 'n' are decomposed into functions at level 'n+1' [4].

Both these techniques are standard in system risk analysis, serving the purpose of providing a qualitative picture of the nominal physical behaviors of the plant components jointly with their mutual functional and hierarchical relations. The results of the application of these techniques feed the successive phases of the methodology: the unambiguous definition of the functions expected from the components implicitly defines what they should not do (i.e., the possible deviations from the nominal behavior), whereas the clear identification of their interfaces (input, output, environment, etc.) allows the identification of the 'cause/effect' elements, at any indenture level, that in case of failure are affected by or could affect the considered components; this is, then, the input for the identification of the failure modes, effects and causes of the components.

3.2 Identification of hazards and failure analysis

Hazard is here defined as any real or potential condition that may result in a business interruption or may cause damage to or loss of assets. Therefore, hazards are not events, but are threats to assets and production that if triggered by specific initiator events have negative effects on the exposed properties, but if opportunely managed do not lead to any accident. The aim is then that of identifying effective methods for assisting engineers in coping with the hazards, i.e. in spotting out, classifying, eliminating and/or controlling them. Again, we remark that 'safety-related' hazards, i.e., that may result in injury, illness, or death to personnel or damage to the environment are not taken into account in this analysis.

Figure 4 sketches the conceptual framework of the analysis. The first step is the investigation of how and to which extent occurrences of failure events and/or deviations of process parameters can lead to business interruption and loss of assets. This step has been performed by thoroughly applying the HAZard IDentification method (HAZID) in successively refined and detailed design settings. HAZID is a qualitative, structured and iterative process commonly used in the framework of safety analyses ([6]-[8]). In our work, it has been adapted to the specification of identifying hazards to structures, systems and components and to qualitatively evaluating probabilities and potential consequences on production and assets, should the hazards actually be activated.

With regards to the synoptic of Figure 4, the hazards in each area of the plant are first searched by a checklist of hazards (Preliminary Hazard List, [6] and [7]), prepared by a team of competent engineers coming from a mixture of disciplines and led by the risk analysts, experienced in the use of the HAZID technique. The preparation of the list reflects the experts knowledge, their lessons learnt and available standards (e.g., [4] and [7]). Notice that external hazards (earthquakes, tornadoes, sandstorms, etc.) have not been considered in the analysis, as both their frequency and magnitude heavily depend on the site of plant installation.

Where it is agreed that an hazard exists in a particular area (i.e., an 'Hazard Manifestation' has been recognized [4]), then the corresponding initiator event (i.e., an event that unleashes the potential inherent cause of the hazard and, either directly or indirectly, results in a damage to assets or loss of production) is

identified jointly with its possible causes. Initiator events should be hunted out among the possible failures and defects of components, software errors, human errors, etc. Experts experience, lessons learnt, collection of failure data (e.g., [10], [11]) are again the knowledge sources that feed this part of the study. Notice that an hazard could be triggered by different initiator events leading to identical or different consequences.

Once an hazard has been activated, the hazard scenario, which reflects the chain of events from causes to final effects, is outlined and the impact that these effects have on production and assets is evaluated. This entails investigation of the physical and functional layout of the systems and components of the plant, assessment of the mechanisms involving physical damage or functional failure propagation, and description of the physical and functional behaviors of systems and components in case of occurrence of the initiator events (the previous step of system understanding, functional and logical description aids such investigation). In particular, combinations of faults undetected before the initiator event, failures of the operator to act on demand, failures of components to operate throughout a specified interval, components unavailability due to testing or maintenance, dependent failures, concurrent activations of other hazards etc. should be considered in the definition of the hazard scenarios ([6], [8] and [9]).

The frequency of occurrence of the triggering event and the severity associated to the consequences of the hazard scenario provide the basis for making the final decision about risk acceptability: this can be achieved by resorting to a risk matrix evaluation ([5], [8], [12]).

A number of peculiarities, tailored to the objectives of the work, characterize this part of the analysis. First of all, the criteria used for deriving the risk matrix are innovative. More specifically, both the magnitude and frequency levels defining the risk criteria have been selected taking into account the expected lifetime and the estimated yearly revenues from the operation of the reference CSP plant. From the simulation performed considering the typical meteorological year for a selected representative site and the actual electric energy tariffs, the X-ITE® performance figures show a net yearly income of about 12.5 M€. Consequently, the risk levels have been tuned with reference to such value: an expected risk of business interruption and asset loss above this figure the risk is considered "High" (≥ 12.5 M€) and "Very High" if ten times this figure (≥125 M€). On the other hand, if the expected risk is lower than 1.25 M€ it is considered "Low" and "Medium" in-between. The individual severity and the frequency levels have been selected so as to obtain these limits (Table 1).

Secondly, the frequency of occurrence relates to the initiator event instead of the final accident sequence. This approach is practical and conservative in that it leads to an over-estimation of the risks associated to the hazard scenarios; in fact, unless the initiator event is a Single Failure Point (SFP, i.e. the failure results directly in the final effect and is not compensated for by redundancies, alternative operational procedures, etc.), the hazard scenario is typically made up of a sequence of events (that may or may not occur) of frequency smaller than that associated to the first event of the sequence (details about the computation of the probability of sequences of events can be found in [8], [9], [12]). Moreover, the frequencies of the initiator events considered can be derived from commercial databases and entirely assigned to the failure modes that trigger the corresponding hazards; this also results in a conservative estimation of the frequencies of the initiator events because, actually, the frequencies should be apportioned among the different failure modes of the components and de-rated depending on the actual operating time, which is just an aliquot of the calendar mission time, e.g. because parts of the CSP plants do not work nightime.

Finally, the quantification of the loss of assets corresponding to a given scenario is based on expert opinion whereas the estimation of the economic losses due to business interruptions is computed by multiplying the expected annual income from plant operation by the expected unavailability due to stoppage; both these estimations are made conservatively and lead to an over-estimation of the severity assigned to the hazard scenarios.

The reasons for applying such conservatisms are driven by the peculiarity of the practical framework in which the analysis is performed. Process and design parameters, failure behaviors of the components, etc., are all affected by unknown uncertainties, which affect the final results of the analysis. On the other hand, the objective of the analysis is to provide elements of confidence to the investor about the performance of the plant, which conservatism can aid.

The hazard scenarios which from the analysis turned out acceptable (i.e., of Medium and Low risk), lead at most to sustainable economic losses and do not need further investigations. On the contrary, a thorough quantitative analysis is required for those hazard scenarios which have come out unacceptable, aimed at an accurate estimation of the frequency of occurrence and magnitude of their consequences, in terms of losses of production and assets.

Table 2 presents a snapshot of the HAZID method applied to the CSP plant object of the present study. 'Electrical Energy' is the hazard considered in the first row of Table 2; this manifests itself in the Solar Field and more precisely in the orientation system (i.e., the system that moves the parabolic collectors in order to track the Sun). A failure in the electrical network, caused by accidental events outside the plant, is the event that triggers the hazard scenario. This results in a black-out longer than 5-6 minutes, which is the time estimated by the expert for the molten salt to exceed the temperature safety limit of 600°C (mishap). The frequency of occurrence of this type of failure is inferred from data collected by the Italian electrical distribution utility. The high temperatures reached in this scenario damage the troughs and the final collector loops: this is the effect associated to the scenario. Considering the part of the plant which is exposed to this effect, an evaluation of the losses of production and assets is obtained.

The HAZID method applied for the analysis of the CSP plant, has led to the identification of 113 hazard scenarios: 67 of these are associated to a Low risk level, 20 to a Medium risk level, 16 are unacceptable (15 with an High risk level and 1 Very High): these scenarios, reported in the Critical Hazard List (CHL) of Table 3, have been subjects of detailed investigations in the successive phase of the methodology.

3.3 Quantitative Analysis

Based on the results of the hazard identification step, the proposed methodology focuses on the detailed quantitative analysis of those scenarios which have turned out not acceptable (Figure 4). The analysis aims at calculating more accurately the values of frequencies and severities assigned to initiator events and consequences, respectively. If the risk associated to the hazard scenarios is still not acceptable after performing the detailed, quantitative analysis, then an hazard reduction process is in order, to eliminate, reduce or control the hazard. In general, the detailed analysis identifies the vulnerable points upon which to act for hazard reduction, e.g., by removal of specific potentially threatening system characteristics, reduction of the amount of specific threats, prevention/reduction of the occurrence of undesired events and/or mitigation of their effects. For example, with reference again to the hazard 'Electrical Energy' of the HAZID Table 2, complete hazard elimination (no electrical energy input) is not possible whereas the issue of hazard reduction (a more reliable electrical network) cannot be addressed by the design of the plant, and hazard prevention may be obtained by the insertion of redundancies or fail-safe systems in the design.

For the systematic risk analysis and communication, each scenario of the CHL is reported in a Worksheet that contains the relevant information on the analysis and its results; this Worksheet is the input to design engineers for considerations of plant improvements. For example, the Worksheet associated to the hazard scenario of the HAZID in Table 2 is shown in Table 4. Its upper part recapitulates the main characteristics of the hazard scenario: the hazard manifestations at different indenture levels, the title name assigned to the hazard scenario, the current situation of the study (i.e., 'opened' when the hazard scenario has been identified; 'confirmed' when a team of experts has validated the plausibility of the hazard scenario; 'closed'

when the quantitative analysis has been performed all the way to verification of the acceptability of the risk and/or hazard reduction measures have been identified).

In the middle part of the Worksheet, the hazard scenario is further detailed; in the example of Table 4, the physical description of the hazard scenarios reads that the stop of the orientation system is due to an electrical black-out and leads to tube ruptures only if the solar radiation is larger than a critical threshold of 600 W/m^2, considering that the sun motion requires almost 3.5 minutes to move out of the direct radiation zone, and if also the back-up energy system is failed.

The feared events are summarized in the successive part of the Worksheet. In the hazard scenario considered in Table 4 there is no feared event at component level; in fact, the component in this case is the orientation system which is not in a fault status, it is simply not energy-supplied. On the contrary, at asset level there is the feared event of rupture of the tubes due to the high temperatures reached by the molten salt mixture (which is not flowing, as also the pumps are not supplied), and from the point of view of production loss the feared event is a significant decrease in power generation performance.

In the Worksheet, it is also important to indicate the identified possible causes that concur in determining the occurrence of the initiator event, to steer the design toward devising solutions for eliminating or controlling them. To this aim, a detailed summary of the characteristics of the hazard scenario is provided; the frequency and severity levels of the scenario guide the direction towards which the analysis effort should be driven. 'Frequency-driven' critical scenarios (those with high frequency levels) call for an investigation of the actual sequence of events leading to the final effect, whereas 'severity-driven' scenarios require a detailed evaluation of the exposure of production and assets. Two elements of relevance for such analyses, and the associated fallbacks onto design are the propagation time and the detectability of the failures in the scenario. The latter indicates the capability of the current design under analysis of detecting the unleashing of the chain of undesired events; the former provides a measure of the time span between the occurrence of the initiator event and the realization of the consequences: a 'yes' in the corresponding cell of the Worksheet signifies that there is enough time to act on the sequence of events that constitute the scenario, before its final effects are realized.

The concluding section of the Worksheet details the quantitative investigations performed for the scenario considered. In particular, for the scenario in the Worksheet of Table 4, a first investigation consists in a refined estimation of the severity of the business interruption and loss of assets consequent to the considered scenario. In particular, the simpler and conservative initial analysis has been substituted by a detailed dynamic simulation, which takes into account the different positions of the individual receivers in each collector loop. In fact the receivers have different initial temperatures, ranging from 290°C to 550°C, and thus different exposition times needed to reach the temperature limit. Another effect that has been considered is that the temperature increase rate is lower at high temperatures. As a result of the detailed simulation study performed, the estimation of the severity of business interruption and loss of assets turns out drastically reduced, but not sufficiently to reach the safe zone (i.e., Medium and Low risk). A second investigation consists in a detailed probabilistic analysis for estimating the frequency of occurrence of the final accident consequent to the hazard scenario under analysis: in the example of Table 4, this accident is treated as the top event of the Fault Tree (FT) that models the logic relations of the events involved in the hazard scenario (assumptions and explanatory comments on the analysis are provided in the Worksheet). In the case at hand, the Fault Tree Analysis (FTA) has been performed by using the BlockSim® software tool, and verified by independent calculations. Typically, the Worksheet ends with a number of final recommendations for consideration by the designers and decision makers.

The complete quantitative analysis of the 16 critical scenarios of the CHL has taken back to an acceptable level the risk estimated for 15 of them. The only hazard remaining critical is the Water Hammer scenario,

whose Worksheet is reported in Table 5. In this case, the current level of design details does not allow to assess (via simulation tools) the plausibility of the occurrence of such phenomenon nor the extent to which the assets are exposed to its effects. This highlights the added value of the systematic analysis performed, which has enabled the identification of an issue that must be carefully addressed and verified in the design of the plant hydraulic system.

Finally, a remark seems in order to underline that all quantitative analyses performed are conservative in that the assumptions made for the estimation of both the probabilities of occurrence of the accidents and the corresponding effect severities have been cautiously taken towards values larger than the expected ones.

4 Conclusions and future works

A methodology has been built on the framework of system risk analysis, to assess the economic sustainability of a CSP plant of innovative design with respect to the risks related to the occurrence of events that can lead to business interruption and/or loss of assets. The application of the methodology has been shown with reference to a real design currently under consideration for investment by Techint. The qualitative analysis step of the methodology, based on over-conservative expert considerations, has revealed the presence of 113 hazard scenarios, of which 16 are potentially leading to an unsustainable economic risk.

The outcome of this step of the analysis has required a further step of detailed, quantitative analysis of these 16 critical scenarios, for an accurate estimation of the risks they actually pose. The results of the quantitative analysis have shown that 15 of the critical scenarios actually lead to an acceptable level of risk. One scenario, that of water hammer, has been left open for careful considerations by the designers of the hydraulic system, for its prevention and/or the control of its effects.

The introduction of detailed worksheets to report the quantitative analyses has proved to provide an effective tool of risk communication, clearly depicting the scenario, its analysis and outcomes, thus providing the design engineers with indications and recommendations useful for the improvement of the system reliability and the economic sustainability of the plant (e.g., attention to be paid in the hydraulic system for avoiding water hammers, sufficiency of one back-up Diesel engine instead of two, etc.); this can bring a significant added value.

The proposed methodology is based on a top-down approach of investigation, which can be further complemented by bottom-up analysis (e.g., a Failure Mode Effects and Criticality Analysis) for a systematic and complete search of initiator events.

The methodology is also prone to tailoring for application to different technological installation sites and projects, leading to the perspective of its extension as a ‘Company Tool’ for the analysis of the performances of plants and systems designed or installed in various fields of application (power transmission, nuclear plants, etc.).

5 References

[1]. Communication from the European Commission to the European Council and the European Parliament from 10 January 2007 “An energy policy for Europe”. (2007)

[2]. European Commission, Directorate - General for Energy and Transport & Directorate - General for Research: Concentrating Solar Power from research to implementation. (2007)

[3]. DI-GDRQ-81223, Schematic Block Diagram.

[4]. ECSS-E-10-05A, Functional Analysis. (1999)

[5]. MIL-STD-1629, Failure Modes and Effect Criticality Analysis. (1980)
[6]. ECSS-Q-40-02A, HazardAnalysis. (2003)
[7]. MIL-STD-882C, System Safety Progam Requirements. (1993)
[8]. PRA Procedure Guide, Vols 1&2, NUREG/CR-2300. (1985)
[9]. Pobabilistic Risk Assessment Procedure Guide for NASA Managers and Practitioners, NASA. (2002)
[10]. NPRD -95, Non Electronic Reliability Data. (1995)
[11]. Guidelines for Process Equipment Reliability Data, with Data Tables. Center for Chemical Process Safety (CCPS) February 1989. Wiley.
[12]. Zio E.: 'An introduction to the basics of reliability and risk analysis'. World Scientific. (2007)

6 Figures

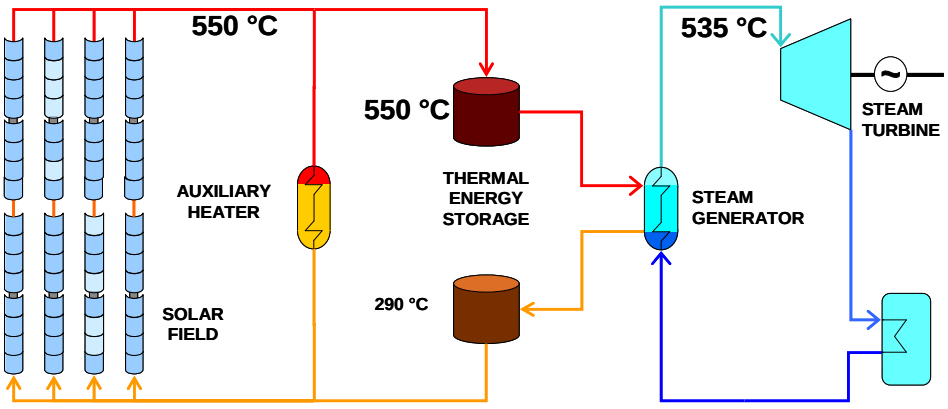


Figure 1: scheme of the X-ITE through parabolic collector solar plant

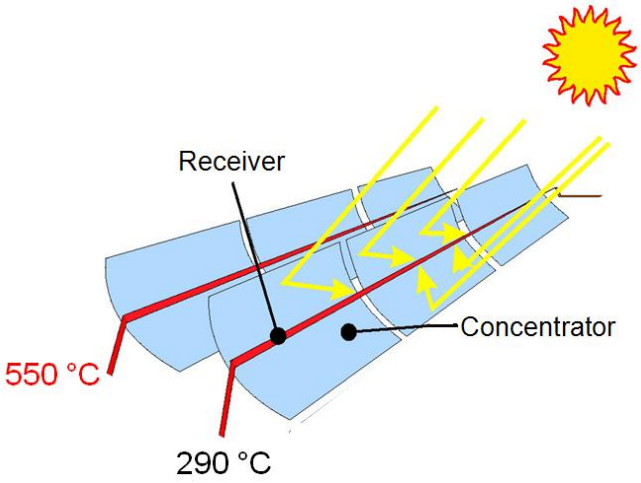


Figure 2: parabolic solar collectors

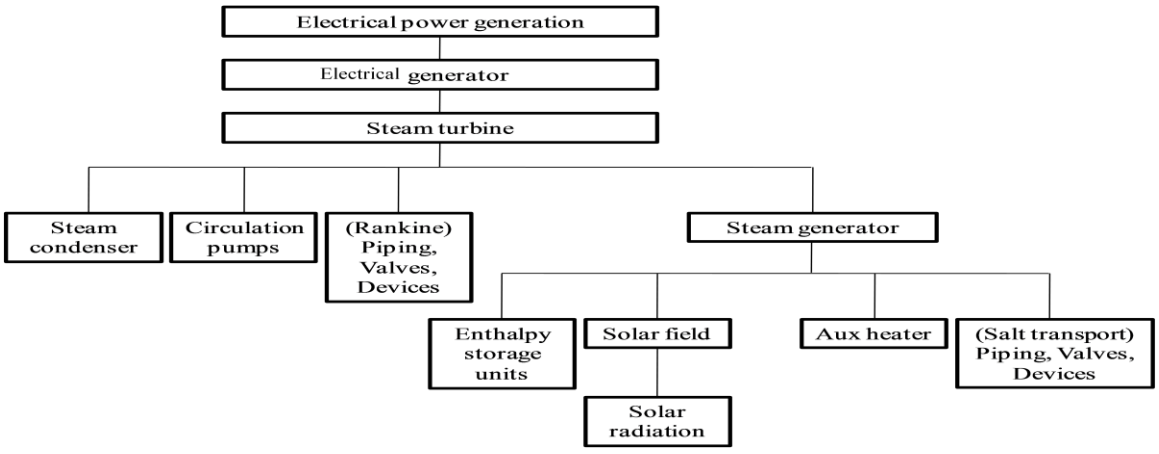


Figure 3: X-ite trough plant block diagram

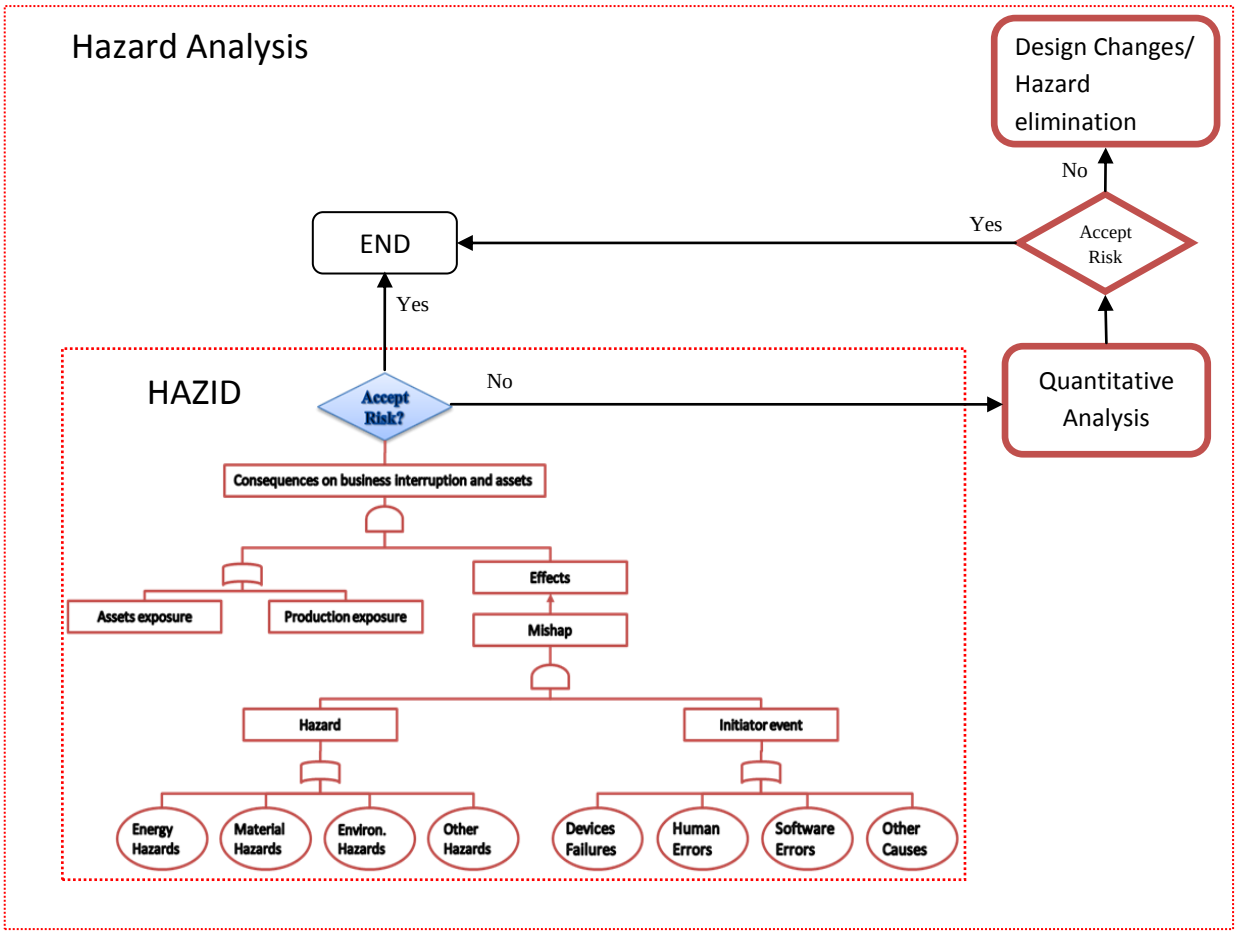


Figure 4: synoptic of Hazard Analysis

7 Tables

Table 1: Risk Matrix

Severity						Risk level	
Very High>	5,000,000					<= 12500	Low
High <	5,000,000	1,250,000	12,500,000	125,000,000		<= 1250000	Medium
Medium <	500,000	125,000	1,250,000	12,500,000		<= 12500000	High
Low <	50,000	12,500	125,000	1,250,000		>= 125000000	Very High
		0.25	2.50	25.00	25.00	[events/MisionTime years]	
		0.01	0.1	1	1	[events/year]	
		Low <	Medium <	High <	Very High>	**Frequency Level**	

Table 2:HAZID example

ID	Hazard	Hazard Manif.: design detail Level 1	Hazard Manif.: design detail Level 2	Hazard Scenario: Primary causes	Hazard Scenario: Initiator event	Hazard Scenario: Mishap	Hazard Scenario: Effect	Potential consequences (asset)	Potential consequences (prod.)	Init. Event Freq. [y^{-1}]	M (prod)	M (asset) level	M (tot.)	R	Existing safeguards
30	Elecrical Energy	Solar field	Orientation system	External events	Failure in the electrical network longer than 4÷5 minutes	Overheating due to stop of salt circulation with solar field blocked on focus	Trough failure and over-temperature on all final collectors loops	Rupture of tubes	Loss of performance	0.03000	9,000,000	8,000,000	9,800,000	7,350,000 (High)	Status signal of pump failure Skin high temperature alarm

Table 3: Critical Hazard List (CHL)

ID	Title	Frequency	Severity	Risk
30	Orientation system stopped	High	High	Very High
20	Water Hammer	Very High	Medium	High
125	Turbine Failure	High	High	High
131	MV Switchgear tripping	High	High	High
83	Low pumping (SG pumps)	High	High	High
88	Salt solidification due to no pumping	High	High	High
42	No pumping (Solar Field)	High	High	High
90	Salt solidification due to no flow	High	High	High
73	Steam Generator Internal Leakage	High	High	High
124	Turbine Leakage	High	High	High
23	Salt solidification due to loop isolation	High	High	High
24	Salt solidification due to prolonged bad weather conditions	High	High	High
25	Salt solidification due to failure of three pumps	High	High	High
26	Salt solidification due to short Power Failure (cold spots)	Medium	High	High
27	Salt solidification due to prolonged Power Failure	Medium	High	High

Table 4: example of Worksheet

Project:	X-ite trough parabolic collectors solar plant	Worksheet 1
System:	Solar Field	SITUATION opened on: 25/03/2010 confirmed on: 12/04/2010 closed on: 10/05/2010
Component	Orientation System	
Number of HAZID Row:	30	
Title:	Orientation System stopped	

Hazard Type: Electrical Energy

Description of sequence of events:

- Black-out of the electrical network
- Back-up system failed
- With the Trough on focus the sun motion requires about 3.5 minutes to avoid any further concentration
- The orientation system remains blocked on focus for at least 3.5 minutes with solar radiation above a level of 600 W/m^2
- Salt circulation is not possible

Feared events:

At component level	No damages
At asset level:	Trough failure/Rupture of ¼ of Receiver Tubes (those ones at higher temperature)
Loss of performance	Large

Possible causes:

Failure in the electrical network.

Level of severity:	High	**Level of frequency**:	Very High	**Detectability** (yes/no):	Yes
SFP : (yes/no):	NO	**Propagation Time**:	Yes		

Further investigations

A more detailed evaluation of the asset losses and business interruption has been performed considering the different initial temperatures of the Receiver Tubes.

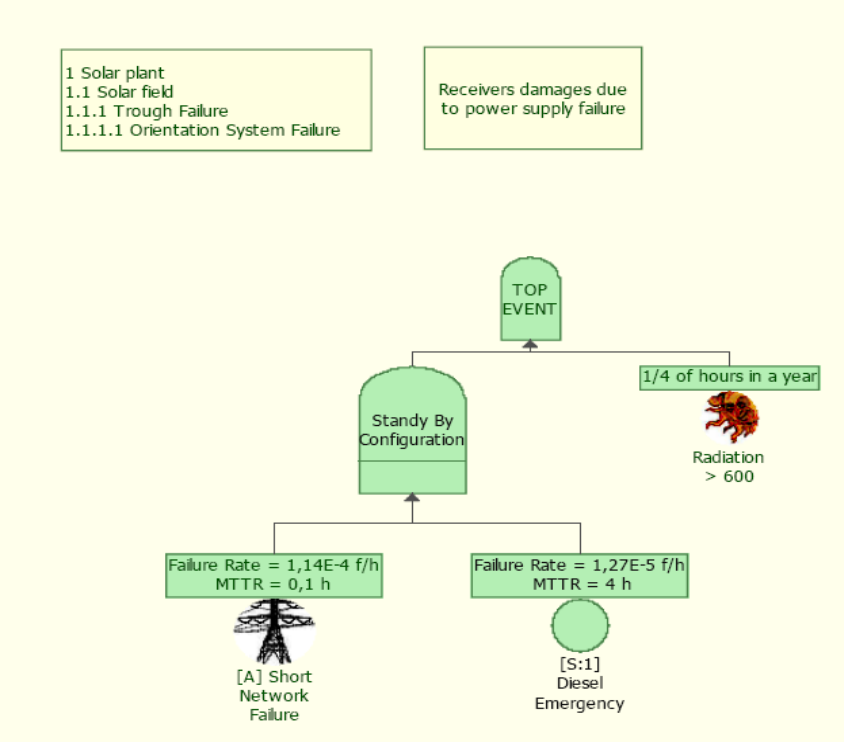
		Temperature at manifold output [°C]					
Solar Radiation		550.0	506.7	463.3	420.0	376.7	333.3
	200	0.15	0.27	0.40	0.52	0.62	0.66
	400	0.47	0.53	0.60	0.66	0.70	0.72
	600	0.58	0.62	0.66	0.70	0.74	0.75

	800	0.64	0.66	0.70	0.73	0.75	0.76
	1000	0.66	0.69	0.72	0.74	0.76	0.77
		290	550	43.333333			
Solar Radiation [W/m2]		Input Power per linear meter of mirror [W/ml]					
	200	177.0	318.6	472.0	613.6	731.6	778.8
	400	1109.2	1250.8	1416.0	1557.6	1652.0	1699.2
	600	2053.2	2194.8	2336.4	2478.0	2619.6	2655.0
	800	3020.8	3115.2	3304.0	3445.6	3540.0	3587.2
	1000	3894.0	4071.0	4248.0	4366.0	4484.0	4543.0
Solar Radiation [W/m2]		Transition time toward the next temperature level [min]					
	200	42.37	20.40	13.77	10.59	8.88	8.35
	400	6.76	5.20	4.59	4.17	3.93	3.83
	600	3.65	2.96	2.78	2.62	2.48	2.45
	800	2.48	2.09	1.97	1.89	1.84	1.81
	1000	1.93	1.60	1.53	1.49	1.45	1.43
Solar Radiation [W/m2]		Time to failure [min]					
	200	42.37	62.77	76.55	87.14	96.02	104.37
	400	6.76	11.96	16.55	20.72	24.66	28.48
	600	3.65	6.61	9.40	12.02	14.50	16.95
	800	2.48	4.57	6.54	8.42	10.26	12.07
	1000	1.93	3.52	5.05	6.54	7.99	9.42

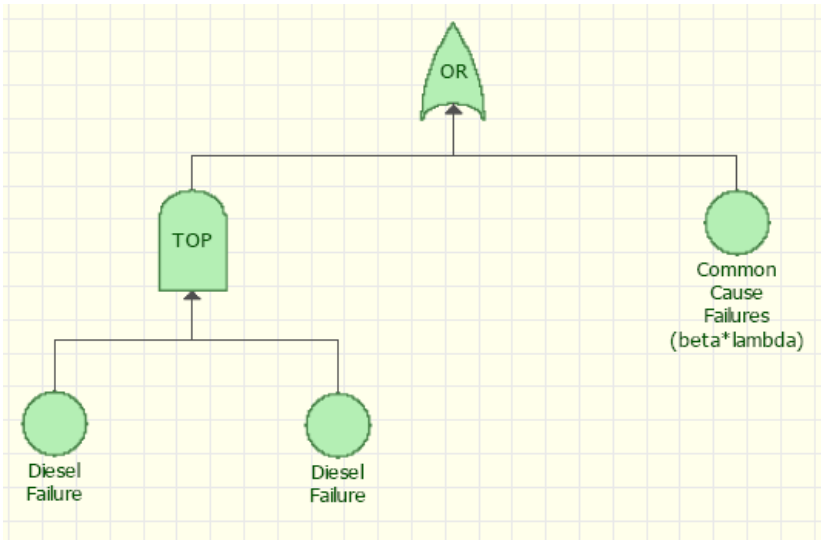
Assumptions
27 percent of time with solar radiation > 600 W/m2 1900 modules of 12 meters 1400 euro per trough + 300 maintenance = 1700 euro 0.7° to exit from focus Solar angular speed NS .204°/min 3.43 minutes to exit from focus

		0.649	-		
	200	0.037	-		
	400	0.047	-		
	600	0.078	0.167	0.01	0.05
	800	0.073	0.167	0.01	0.05
	1000	0.116	0.333	0.04	0.14
		1.000	0.667	0.06	0.24
	1/4 of broken troughs				
	2,422,500				

The occurrence frequency of the event ‘trough failure’ has been computed by the following Fault Tree (FT).



where the failure rate and the mean time to repair (MTTR) of the 'Diesel Emergency' event are given by the following FT



Assumptions:

a) There are two diesel engines which are back-up systems of the nominal energy supplier i.e., the electrical network. In particular, the two engines are arranged in a cold stand-by with perfect switch configuration (see [12]).
b) It has been assumed that both diesel engines are periodically inspected with a period τ=3 months. In particular, inspection procedures (testing and maintenance) have been supposed to take 1h and be perfect.
c) The probability of failure on demand, *f*, of the engines when requested to start is not known; thus, it has not been taken into account. This leads to an under-estimation of the diesel engines failure

probability, but this is considered negligible.

d) Common Cause Failures for the two diesel engines have been taken into account by applying the Beta-factor model with a conservative value of β=0.1.
e) The failure rate of the electrical network refers to the Italian electrical distribution network.

Results of the Fault Tree Analysis (FTA):

$MTTFF=25276\ 10^3\ h$

On this basis, the risk level associated to the present hazard scenario turns out to be acceptable.

Given the very high value of the MTTFF, the FTA has been repeated considering only one back-up Diesel engine. The result in this case is:

$MTTFF=19990\ 10^3\ h$

Therefore, even with only one Diesel engine the risk level associated to the present hazard scenario comes out to be acceptable.

Recommendations:

a) Skin high temperature alarm and the status signal of pump failure are safeguards only if they work even in case of power failure; thus, they should have an independent power source (e.g., battery).
b) Evaluate the option of developing a system which in case of electrical black-out automatically moves the mirrors from the maximum radiation position.
c) The diesel engine needs to be tested periodically (at least every third month).

Signature and date

Table 5: water hammer hazard scenario

Project:	X-ite trough parabolic collectors solar plant	Worksheet 2
System:	Solar Field	SITUATION opened on: 25/03/2010 confirmed on: 12/04/2010 closed on: 10/05/2010
Component	Pumps	
Number of HAZID Row:	20	
Title:	Water Hammer	

Hazard Type: Fluid Flow

Description of sequence of events:

- Sudden pump stop
- Creation of a water hammer

Feared events

At component level	Failure (jamming) or sudden stop of the electrical supply
At asset level:	Damages of pipes, valves, pumps etc.
Loss of performance	Large

Possible causes:

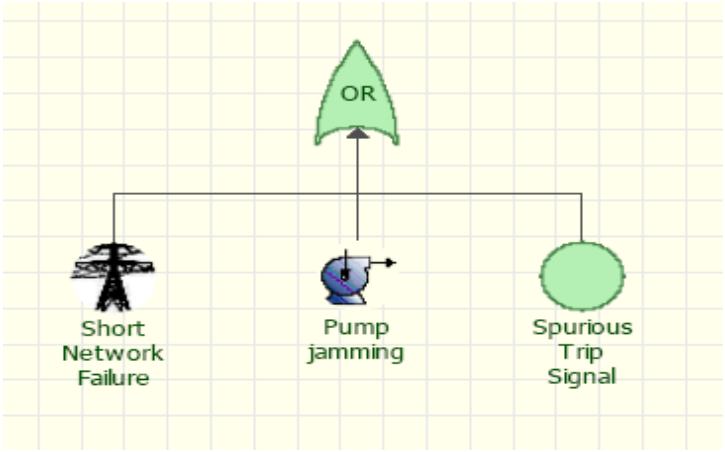
Failure in the electrical network and failure of the back-up systems (diesel engines). Stuck due to grips, powders, etc.

Level of severity:	Medium	**Level of probability**:	Very High	**detectability** (yes/no):	No
SFP : (yes/no):	Yes	**Propagation Time**:	No		

Further investigations: Water hammer (or, more generally, fluid hammer) is a pressure surge or wave caused by the motion of a fluid when it is forced to stop or change direction suddenly. It can generate a very destructive force that can break or damage the pipe or even the equipment of an hydraulic system. It is caused by a pressure or shock wave that travels faster than the speed of sound through the pipes, brought on by a sudden stop in the velocity of the water, or a change in the direction. The FT reported in this Sheet can be used to compute the frequency of occurrence of a sudden stop of the fluid. However, two questions arise:

1. The failure rate of the basic event 'Spurious Trip Signal' is not known;
2. A sudden stop may not generate a water hammer.

Therefore, further investigations of the hydraulic circuits of the plant will be performed in order to verify the plausibility of the generation of water hummers and to suggest possible preventions and mitigation actions. This may reduce or even eliminate the risks related to the sudden fluctuation of pressure generated by the phenomenon.



Signature and date